

## AMENDMENTS

1. (Currently Amended) An apparatus for sealing a data repository to a trusted computing platform, the apparatus comprising:
  - an embedded security system (ESS) comprising at least one platform configuration register;
  - a measurement module configured to generate one or more measurement values for one or more devices physically connected to a computer system and to extend the measurement values to at least one platform configuration register;
  - a key management module configured to seal a cryptographic key associated with a data repository by cryptographically combining the cryptographic key with the measurement values for one or more of a BIOS, a boot record, a drive serial number, and an object code image of decryption software in at least one platform configuration register, the measurement values representing a trusted configuration of the trusted computing platform, and to unseal the cryptographic key using the measurement values by way of the ESS; and
  - a cryptography module configured to encrypt data stored in the data repository and to decrypt data read from the data repository with the unsealed cryptographic key.
2. (Canceled)

3. (Previously Presented) The apparatus of claim 1, wherein the ESS is a Trusted Platform Module (TPM).
4. (Currently Amended) A system for sealing a data repository to a trusted computing platform, the system comprising:
- a data repository configured to encrypt data written to the data repository and to decrypt data read from the data repository using a cryptographic key;
  - an embedded security system (ESS) comprising at least one platform configuration register;
  - a measuring module configured to generate one or more measurement values for one or more devices within the system and to extend the measurement values to one of the at least one platform configuration registers; and
  - a key management module configured to:
    - seal the cryptographic key associated with the data repository by cryptographically combining the cryptographic key with the at least one platform configuration register measurement value for one or more of a BIOS, a boot record, a drive serial number, and an object code image of decryption software, the measurement value representing a trusted configuration, and to unseal the cryptographic key using the measurement values by way of the ESS; and

read a sealed cryptographic key, unseal the cryptographic key, and provide the cryptographic key to the data repository before an operating system loads.

5. (Previously Presented) The system of claim 4, wherein the ESS is a Trusted Platform Module (TPM).

6. (Original) The system of claim 4, wherein the key management module is further configured to write the sealed cryptographic key to a non-volatile data repository and to read the sealed cryptographic key from a non-volatile data repository.

7. (Original) The system of claim 6, wherein the non-volatile data repository is a repository selected from the group consisting of an unencrypted partition of a hard drive, a removable device, and a removable media.

8. (Canceled).

9. (Currently Amended) A computer readable storage medium comprising computer readable code configured to carry out a method for sealing a data repository to a trusted computing platform, the method comprising:  
encrypting data on a data repository with a cryptographic key;  
sealing the cryptographic key by cryptographically combining the cryptographic key with measurement values for one or more of a BIOS, a boot record, a drive serial number, and an object code image of decryption software, the measurement values

representing a trusted configuration to a platform configuration to  
produce a sealed key;  
unsealing the sealed key using the measurement values to produce the  
cryptographic key; and  
decrypting data on the data repository with the unsealed cryptographic  
key.

10. (Previously Presented) The computer readable storage medium of claim 9, wherein sealing comprises generating a measurement value for a device comprising the platform configuration and generating the sealed key with the measurement value.

11. (Previously Presented) The computer readable storage medium of claim 10, wherein generating a measurement value comprises hashing a code image.

12. (Previously Presented) The computer readable storage medium of claim 9, wherein the sealed key is generated with a Trusted Platform Module (TPM).

13. (Previously Presented) The computer readable storage medium of claim 9, wherein unsealing comprises decrypting the sealed key with a measurement value for a device comprising the platform configuration, the measurement value matching a measurement value used to produce the sealed key.

14. (Previously Presented) The computer readable storage medium of claim 13, wherein a TPM unseals the sealed key.

15. (Previously Presented) The computer readable storage medium of claim 9, further comprising storing the sealed cryptographic key in a removable device.

16. (Previously Presented) The computer readable storage medium of claim 9, wherein the platform configuration comprises a serial number for the data repository.

17. (Previously Presented) The computer readable storage medium of claim 9, wherein the platform configuration comprises a decryption module.

18. (Previously Presented) The computer readable storage medium of claim 9, wherein the platform configuration comprises firmware and software accessible to a processor without the sealed key.

19. (Currently Amended) A method for sealing a data repository to a trusted computing platform, the method comprising:

- encrypting data on a data repository with a cryptographic key;
- sealing the cryptographic key by cryptographically combining the cryptographic key with measurement values for one or more of a BIOS, a boot record, a drive serial number, and an object code image of decryption software, the measurement values representing a trusted configuration to a platform configuration to produce a sealed key;
- unsealing the sealed key using the measurement values to produce the cryptographic key; and

decrypting data on the data repository with the unsealed cryptographic key.

20. (Previously Presented) The method of claim 19, wherein sealing comprises generating a measurement value for a device comprising the platform configuration and generating the sealed key with the measurement value.

21. (Previously Presented) The method of claim 20, wherein generating a measurement value for a device comprises hashing firmware code for the device.

22. (Previously Presented) The method of claim 20, wherein the sealed key is generated with a Trusted Platform Module (TPM).

23. (Previously Presented) The method of claim 19, wherein unsealing comprises decrypting the sealed key with a measurement value for a device comprising the platform configuration, the measurement value matching a measurement value used to produce the sealed key.

24. (Previously Presented) The method of claim 19, wherein a TPM unseals the sealed key.

25. (Previously Presented) The method of claim 19, further comprising storing the sealed key in a removable device.

26. (Previously Presented) The method of claim 19, wherein the platform configuration comprises a serial number for the data repository.

27. (Previously Presented) The method of claim 19, wherein the platform configuration comprises a decryption module.

28. (Previously Presented) The method of claim 19, wherein the platform configuration comprises firmware and software accessible to a processor without the sealed key.

29. (Currently Amended) An apparatus comprising a logic unit for sealing a data repository to a trusted computing platform, the apparatus comprising:  
means for generating a measurement value for a device among a plurality of devices comprising a platform configuration;  
means for sealing a cryptographic key associated with a data repository to the measurement value for two or more of a BIOS, a boot record, a drive serial number, and an object code image of decryption software, the measurement value representing the device, to produce a sealed key;  
means for unsealing the sealed key; and  
means for decrypting data on the data repository with the unsealed cryptographic key.

30. (Currently Amended) An apparatus for sealing a data repository to a trusted computing platform, the apparatus comprising:

- an embedded security system (ESS) comprising at least one platform configuration register and configured to seal a cryptographic key to platform configuration data stored in the at least one platform configuration register to produce a sealed key and further configured to unseal the sealed key to produce an unsealed cryptographic key;
- a key management module configured to direct the ESS to seal a cryptographic key associated with a data repository by cryptographically combining the cryptographic key with a measurement value for a drive serial number associated with the data repository, the measurement values representing a trusted configuration of the trusted computing platform, and further configured to manage the sealed key,
- a measurement module configured to generate the measurement value for the data repository physically connected to the ESS, the ESS extending the measurement value to the at least one platform configuration register;
- a cryptographic module configured to encrypt data stored to the data repository and to decrypt data read from the data repository with the unsealed cryptographic key, and
- a removable data repository configured to store the sealed key associated with the data repository.